UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,892	08/10/2006	Naoto Kuroda	9319Y-1322/NP	7169

27572 7590 12/03/2008

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,892	KURODA, NAOTO	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15-18,20 and 21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-18,20 and 21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to filing on 9/19/2008. Claims 1-13, 15-18, 20 and 21 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-13, 15-18, 20, and 21 are rejected under 35 U.S.C. 102 (b) as being anticipated by Arnold et al (US Patent No. 5,440,723 and Arnold hereinafter).

2. As to claim 1, Arnold teaches a method of preventing virus infection by detecting the virus infection in a network, comprising steps of:

obtaining communication information when a virus intrudes (i.e., … teaches obtaining virus signature information [col. 9, lines 10-20]); detecting a virus source computer based on the communication information obtained (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer

network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

sending a message announcing an antivirus attack on the virus source computer [fig. 3, (E)];

and making the antivirus attack on the virus source computer [fig. 5, Block A-E].

3. As to claim 2, Arnold teaches a method of preventing virus where:

a decoy accessible through the network is provided to a computer that monitors intrusion of a virus (i.e., ... teaches deploying a decoy to capture virus [item C, fig. 2]), for receiving access to said decoy to obtain communication information and to detect virus intrusion (i.e., … teaches the DPs are periodically compared to the secured copies stored within the DPDB 76a so as to detect a modification thereof [col. 29, lines 8-12]);

and said decoy is one or more of a decoy folder stored in a storage unit, a decoy application stored in the storage unit (i.e., teaches the decoy program unit 76 has an associated secure decoy program database (DPDB) 76a [col. 29, lines 1-10]), and a server formed virtually in the storage unit (i.e., … although silent on the term “server”, those ordinary skill in the art would recognize the teaching of the DPs are periodically compared to the secured copies stored within the DPDB 76a so as to detect a modification thereof. If a modification is detected, the DPU 76 isolates the undesirable software entity and provides one or more samples of the isolated undesirable software entity to the code/data segregator 38 [col. 29, lines 8-16]).

4. As to claim 3 and 8, Arnold teaches a method of preventing virus infection where: said attack is made by imposing a high load on the virus source computer (i.e., … teaches anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse [col. 4, lines 30-35]).

5. As to claim 4 and 9, Arnold teaches a method of preventing virus infection where: said high load is imposed on the virus source computer by increasing traffic of said computer (i.e., … teaches anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse [col. 4, lines 30-35]).

6. As to claim 5 and 10, Arnold teaches a method of preventing virus infection where: said high load is imposed on the virus source computer by sending a large number of requests to which a CPU of said computer should respond (i.e., … teaches anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse [col. 4, lines 30-35]).

7. As to claim 6, Arnold teaches a system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus (fig. 5, Blocks A-E);

and a message sending means that sends a message for announcing a start of the attack, to the infected computer (i.e., … teaches a distress signal deployment [col. 20, Step G]).

8. As to claim 7, Arnold teaches a system for preventing virus infection where:

said system further comprises a decoy means accessible through the network [fig. 2, (C)];

and said communication information analysis means detects virus intrusion into said decoy means, and on detection of the virus intrusion [fig. 3, (J)], detects a virus source computer, based on the communication information obtained when the virus intrudes (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]).

9. As to claim 11, Arnold teaches a system for preventing virus infection where: said system further comprises a detection report transmission means that sends a detection report to an administrator of the virus source computer (i.e., … teaches a signature report displayed on device or stored in the database [col. 19, lines 35-45]);

and said computer attack means continues to make the antivirus attack on the virus source computer until a countermeasure against the virus has been completed [fig. 5, block A-E].

10. As to claim 12, Arnold teaches a system for preventing virus infection where said decoy means is a decoy folder realized by an application provided in a decoy server

that is formed virtually in a storage unit of a computer connected to the network (… teaches added as a dedicated decoy program server [col. 4,lines 25-30]).

11. As to claim 13, Arnold teaches a system for preventing virus infection where: said decoy means is a decoy application realized as an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network (i.e., … teaches Deployment of decoy programs to capture virus samples [col. 4, Step C] … teaches one or more decoy programs in an attempt to attract and obtain one or more samples of the unknown virus. The decoy programs could be commercially-available computer programs which are installed on (and are capable of being executed on) the computer system [col. 6, lines 5-15] … teaches added as a dedicated decoy program server [col. 4,lines 25-30]).

12. 14. (deleted)

13. As to claim 15, Arnold teaches a system for preventing virus infection further comprising: an alarm sound generation means that generates an alarm sound in a attacking terminal unit at a start of the attack or after the start of the attack (i.e., … teaches deployment of a distress signal [col. 20, Step G]).

14. As to claim 16, Arnold teaches a system for preventing virus infection further comprising: a requesting means that notifies a network address of the virus source

computer to another computer connected to the network and requests to said computer for making an antivirus attack on the virus source computer (i.e., … teaches alerting neighboring computers [abstract (F)] … teaches performing antivirus processing [fig. 8] … although silent on the term "request" for making the antivirus attack those skill in the art would recognize upon invoking the process to execute performing antivirus processing in [fig. 8] a triggering process such as a request process would have had to occur for in order for the [fig. 8] processes to execute).

15. As to claim 17, Arnold teaches a system for preventing virus infection by detecting the virus infection in a network, comprising:

a request receiving means that receives a request for making an antivirus attack on a virus source computer … teaches performing antivirus processing [fig. 8] … although silent on the term "request" for making the antivirus attack those skill in the art would recognize upon invoking the process to execute performing antivirus processing in [fig. 8] a triggering process such as a request process would have had to occur for in order for the [fig. 8] processes to execute);

and a computer attack means that makes an antivirus attack on said virus source computer through the network for suppressing operation of a virus, based on said request received [fig., 5, Block A-E].

16. As to claim 18, Arnold teaches a program for making a computer prevent virus infection, wherein: said program makes said computer realize:

a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]):

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus [fig. 5, Block A-E];

and a message sending means that sends a message for announcing a start of the attack, to the infected computer (i.e., … teaches the deployment of a distress signal [col. 20, Step G].

17. 19. (deleted)

18. As to claim 20, Arnold teaches a system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and on detecting virus intrusion, detects a virus source computer, based on

communication information obtained when the virus intrudes (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus [fig. 5, Block A-E];

and an alarm sound generation means the generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack (i.e., … teaches the deployment of a distress signal [col. 20, Step G]).

19. As to claim 21, Arnold teaches a system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and on detecting virus intrusion, detects a virus source computer, based on communication information obtained when the virus intrudes (i.e., … teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a

Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

a detection report transmission means that sends a detection report to an administrator of the virus source computer [fig. 3 (P)].

Prior Art Made of Record

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Lewis et al. (US Patent Publication No. 2003/0110396) Method and apparatus for predicting and preventing attacks in communications networks.

Response to Arguments

21. During the interview conducted on August 6, 2008 applicant's representative pointed out that the claims as examined did not seem to match the claims as amended under article 34. The Examiner agreed that the claims were examined without consideration of the article 34 amendments and suggested that the Applicant for filing a request for reconsideration. Therefore, Examiner respectfully withdraws Non-Final Office action filed on July 16, 2008. Examiner submits claims as file under article 34 amendment on 9/16/2005 has been considered and addressed as described above.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435